

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELLIOTT BROIDY and BROIDY CAPITAL
MANAGEMENT, LLC,

Plaintiffs,

-against-

GLOBAL RISK ADVISORS LLC, GRA MAVEN LLC,
GRA QUANTUM LLC, GLOBAL RISK ADVISORS
EMEA LIMITED, GRA RESEARCH LLC, QRYPT,
INC., KEVIN CHALKER, DENNIS MANDICH,
ANTONIO GARCIA, and COURTNEY CHALKER,

Defendants,

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 3/31/2021

1:19-cv-11861 (MKV)

OPINION AND ORDER
GRANTING MOTION TO
DISMISS

MARY KAY VYSKOCIL, United States District Judge:

This action is at least the fourth attempt by Plaintiff Elliott Broidy and his investment firm Broidy Capital Management (“BCM”) to hold responsible certain actors whom he claims hacked into email servers and then distributed confidential data. Broidy claims that Defendants here were hired by the nation of Qatar to perform the hacking after Broidy’s public condemnation of the country. In other actions, Broidy sued the nation of Qatar itself, a public relations firm and its employees and agents, and a diplomat, all of whom are alleged to have participated in the alleged scheme. This action takes aim at a cybersecurity firm that Broidy alleges did the actual “hacking” of his and his company’s information.

Defendants have moved to dismiss Broidy’s First Amended Complaint on both jurisdictional and substantive grounds. Specifically, Defendants allege that they are either immune from liability due to “derivative foreign immunity” or are not subject to personal jurisdiction here. In addition, Defendants argue that Broidy has failed adequately to plead his

claims and has engaged in improper claim splitting and jurisdiction shopping. For the reasons that follow, Defendant's motion to dismiss is GRANTED.

FACTUAL BACKGROUND

The facts as stated herein are drawn from Plaintiff's First Amended Complaint, ECF No. 57 ("AC"), and are assumed to be true for the purpose of the Motion. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

Plaintiff Elliott Broidy is the Chief Executive Officer and Chairman of BCM. AC ¶ 14. Outside that role, he has long been an active member of numerous political and philanthropic organizations, including serving on the U.S. Department of Homeland Security's Advisory Council, in leadership roles in the Republican Party, and as a major donor to the Joint Regional Intelligence Center. AC ¶¶ 14, 31. Both in these positions and on his own time, Broidy advocates against the nation of Qatar as a state-sponsor of terrorism and, in turn, a threat to U.S. national security. AC ¶¶ 32-34. Broidy further alleges that he was influential in shaping the U.S. stance toward Qatar during the Trump Administration, including by influencing remarks by then-President Trump that Qatar was a "funder of terrorism at a very high level." AC ¶¶ 35-36.

As alleged in the First Amended Complaint, Qatar sought to silence Broidy in an effort to influence U.S. policy regarding relations with the country. AC ¶ 59. To do so, Qatar hired a public relations firm Stonington Strategies LLC and certain others to "develop[] and implement[] a government relations strategy for Qatar." AC ¶ 60. Broidy alleges that the Chief Executive Officer of Stonington Strategies, Nicholas Muzin, "identified and described Mr. Broidy to the Qatari government as impediments to Qatar's foreign policy interests in the United States." AC ¶ 65.

Broidy alleges that upon learning of his role Qatar retained Defendant Global Risk Advisors (“GRA”) to execute a hack of Broidy’s personal systems and those devoted to BCM. AC ¶ 73. Broidy further alleges that Qatar already had a relationship with GRA, after the firm had performed other hacking activities for Qatar, especially in relation to Qatar’s efforts to host the 2022 FIFA World Cup. AC ¶ 68. At Qatar’s direction, GRA designed a “spear phishing” campaign to hack and steal Broidy’s confidential communications.¹ AC ¶ 75.

GRA first targeted Broidy’s wife with spear phishing emails. First, GRA targeted Broidy’s wife, Robin Rosenzweig, through her personal Gmail email address, with emails designed to appear as though they were security alerts sent by Google. AC ¶¶ 77-78. When Ms. Rosenzweig clicked on the links contained in the emails, however, she was redirected to a counterfeit Google login site, which recorded her credentials. AC ¶¶ 79-80. Defendants then used the captured credentials to modify Ms. Rosenzweig’s Gmail account (to prevent her from discovering the hack) and to recover her login credentials to BCM’s servers. AC ¶¶ 81-82.

Defendants executed a similar attack on Broidy’s executive assistant. GRA allegedly sent Broidy’s assistant similar falsified Google security alerts, including at least one with her picture and phone number. AC ¶¶ 84-85. Similar to Ms. Rosenzweig, when Broidy’s assistant clicked on links contained in the email, she was redirected to a counterfeit Google login site where her credentials were captured by GRA. AC ¶¶ 86-87.

After obtaining access to the Gmail accounts of Ms. Rosenzweig and Broidy’s assistant, and using the information it gained from those accounts, GRA gained access to BCM’s servers. AC ¶¶ 88-89. Broidy alleges that GRA and its agents maintained access to the server for

¹ As alleged in the Amended Complaint, “spear phishing” is the “use of fraudulent electronic communication targeted toward a specific individual, organization, or business in order to steal data or install malware on a targeted user’s computer.” AC ¶ 75.

approximately a month in early 2018 and, during that time, accessed attorney-client information, corporate documents, business plans, trade secrets, and other information. AC ¶ 90. Defendants accessed Plaintiffs' servers while masking their IP addresses using Virtual Private Network and Virtual Private Server ("VPN") technologies. AC ¶ 93. However, during a forensic investigation of the hack, Plaintiff determined that hacks were also occurring from IP addresses registered to locations in Vermont (on twelve occasions from two different addresses), Qatar (two occasions from the same address), and, on one occasion, an event space in Harlem, New York City. AC ¶¶ 96-98. Importantly, Broidy alleges that GRA and its agents likely visited the U.S.-based locations only once. However, they obtained remote access to the addresses such that they could physically be located anywhere, but the hacks would be located at the remote locations. AC ¶ 99.

After accessing Plaintiffs' documents, GRA and its agents disseminated them to media outlets and synchronized their efforts with the public relations team at Stonington Strategies. AC ¶¶ 100-107. The materials from the hacks of Plaintiffs' systems were used to lend legitimacy to forged documents and contracts purporting to show Broidy's business dealings with U.S. government-sanctioned companies. AC ¶¶ 109, 111. The forged documents were then reported by media organizations, including Al-Jazeera. AC ¶ 115. Other documents stolen from Plaintiffs' servers were used in media reports in the Wall Street Journal, Huffington Post, Bloomberg, and the New York Times. AC ¶¶ 123-25, 130-31. As a result of the hacks, Broidy and BCM have suffered reputational damage, as business partners have pulled out of existing relationships and have refused to do business with Broidy and his company. AC ¶¶ 136-38.

This case is the latest in a number of litigations Plaintiffs have brought against Qatar and its agents for the reputational and business damage Plaintiffs claim it has caused him through the

alleged hacks and related activities. Broidy and BCM first contacted Qatar in March 2018, about a month after GRA access to BCM's servers was lost, to demand that Qatar stop the hacking attacks. AC ¶ 188. When the country failed to respond, Broidy filed his first case in the United States District Court for the Central District of California, naming as Defendants the nation of Qatar, several Defendants in this action, and others. AC ¶ 189. Upon the filing of that action, Broidy alleges that GRA destroyed evidence relating to its involvement in the hacking enterprise. AC ¶ 190. The California action ultimately was dismissed on the basis of foreign sovereign immunity (as to Qatar) and personal jurisdiction (as to the other Defendants), and the decision was affirmed by the Ninth Circuit.² AC ¶ 191; *see Broidy Capital Mgmt, LLC v. State of Qatar*, 982 F.3d 582 (9th Cir. 2020).

Broidy then filed a case in this District against Jamal Benomar, a former United Nations diplomat whom he alleges aided Qatar in the hacking and public relations conspiracy. AC ¶ 127, 192. That case was dismissed on the grounds of diplomatic immunity, and the dismissal was affirmed by the Second Circuit. AC ¶ 192; *see Broidy Capital Mgmt. v. Benomar*, 944 F.3d 436 (2d Cir. 2019). Finally, in early 2019, Broidy filed an action in the United States District Court for the District of Columbia against Nicholas Muzin and other defendants related to Stonington Strategies. AC ¶ 193. After briefing, the court there denied a motion to dismiss raising many of the same arguments made here. AC ¶ 193; *see Broidy Capital Mgmt., LLC v. Muzin*, No. 19-cv-0159 (DLF), 2020 WL 1536350 (D.D.C. Mar. 31, 2020).

This action was filed in December 2019. *See* Complaint, ECF No. 1. After an initial motion to dismiss the complaint was filed, Plaintiffs filed an Amended Complaint. *See*

² Plaintiffs only appealed the California decision to the extent it dismissed claims against the nation of Qatar on foreign sovereign immunity grounds. They did not appeal from the dismissal of claims against the other Defendants for lack of personal jurisdiction. *See State of Qatar*, 982 F.3d at 589.

Amended Complaint, ECF No. 57. The Amended Complaint asserts claims against ten Defendants whom Plaintiff asserts were involved in the hacking and dissemination of his private communications and documents. They are:

- Global Risk Advisors, LLC (“GRA”) – a Delaware LLC with its principal place of business in New York, NY;
- Several wholly owned subsidiaries of GRA, including:
 - Global Risk Advisors EMEA Limited (“EMEA”) – a Gibraltar corporation;
 - GRA Maven LLC – a Delaware LLC headquartered in Southern Pines, NC that functions as a military consulting firm;
 - GRA Quantum LLC – a Delaware LLC that functions as a cybersecurity company;
 - Qrypt, Inc. – a Delaware corporation with its principal place of business in New York, NY that is involved in cybersecurity operations;
- GRA Research, LLC – a Delaware LLC with offices in Washington, D.C., and Reston, VA;
- Kevin Chalker – the founder and Chief Executive Officer of GRA, domiciled in New York. Plaintiff alleges that Kevin Chalker controls all of the GRA entities (AC ¶¶ 16, 19);
- Denis Mandich – a founder of Defendant Qrypt
- Antonio Garcia – GRA’s Chief Security Officer
- Courtney Chalker – Kevin Chalker’s brother.

AC ¶¶ 14-20, 25-26. The Amended Complaint refers collectively to all Defendants other than Courtney Chalker as the “GRA Defendants.” AC at 1. The Court adopts this definition throughout this opinion. Plaintiff asserts personal jurisdiction in this District on the basis of Defendants’ residence or business contacts. AC ¶¶ 25-26. Subject matter jurisdiction is asserted based on federal question jurisdiction and supplemental jurisdiction over Plaintiff’s state law claims.³ AC ¶¶ 21-22; *see* 28 U.S.C. §§ 1331, 1367.

³ Plaintiff also alleges that jurisdiction is proper based on diversity. *See* 28 U.S.C. § 1332. Broidy and BCM, whose sole member is Broidy, are citizens of California. AC ¶¶ 14-15. However, because Plaintiff has not alleged the membership of all LLC Defendants, diversity jurisdiction is not appropriate here. *See Avant Capital Partners, LLC v. W108 Dev. LLC*, 387 F. Supp. 3d 320, 322 (S.D.N.Y. 2016) (“A limited liability company takes the citizenship of

Plaintiff asserts ten claims against various groups of Defendants. Nine claims are asserted against the GRA Defendants. Five of those claims are predicated on federal statutes, including the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq* (AC ¶¶ 195-209 [Count One]), the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) and (a)(5) (AC ¶¶ 210-24 [Count Two]), the Defend Trade Secrets Act, 18 U.S.C. §§ 1831, 1832, 1836 (AC ¶¶ 225-47 [Count Three]), and the Racketeer Influenced and Corrupt Organizations Act (“RICO Act”), 18 U.S.C. §§ 1962, 1964 (AC ¶¶ 305-404 [Count Nine – Violation of the RICO Act]; AC ¶¶ 405-13 [Count Ten – Conspiracy to Violate the RICO Act]). Plaintiffs also assert three California statutory claims against the GRA Defendants and two common law claims, one of which names Defendant Courtney Chalker: misappropriation of trade secrets under the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426, *et seq.* (AC ¶¶ 248-62 [Count Four]); violation of the California Comprehensive Computer Data Access and Fraud Act, Cal. Pen. Code § 502 (AC ¶¶ 263-76 [Count Five]); receipt and possession of stolen property in violation of Cal. Pen. Code § 496 (AC ¶¶ 277-86 [Count Six]); civil conspiracy (AC ¶¶ 287-95 [Count Seven]); intrusion upon seclusion (AC ¶¶ 296-304 [Count Eight]).

Defendants have moved to dismiss the Amended Complaint [ECF No. 72]. In support of their motion, Defendants filed a memorandum of law, ECF No. 73 (“Def. Br.”) and a declaration of counsel attaching only a copy of Plaintiff’s Amended Complaint, ECF No. 74. Plaintiff opposed the motion with a memorandum of law, ECF No. 76 (“Opp.”). Defendants also submitted a Reply Memorandum of Law, ECF No. 77 (“Reply”). After the motion was briefed, Defendants filed a letter directing the Court’s attention to the Ninth Circuit’s decision in the *State of Qatar* case, 982 F.3d 582, which was filed after Defendants’ motion was briefed. *See*

its members.” (citing *Bayerische Landesbank, New York Branch v. Aladdin Capital Mgmt., LLC*, 692 F.3d 42, 49 (2d Cir. 2012))).

Letter to Court from Orin Snyder dated December 10, 2020, ECF No. 80. Plaintiffs responded to Defendants' letter. *See* Letter to Court from Filiberto Agusti dated December 17, 2020, ECF No. 81.

LEGAL STANDARD

Defendants move to dismiss Plaintiff's Amended Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(2), and 12(b)(6).

Pursuant to Rule 12(b)(1), a district court shall dismiss an action for lack of subject matter jurisdiction when it "lacks the statutory or constitutional power to adjudicate it." *Makarova v. United States*, 201 F.3d 110, 113 (2d Cir. 2000). Where subject matter jurisdiction is challenged, a plaintiff "bear[s] the burden of 'showing by a preponderance of the evidence that subject matter jurisdiction exists.'" *APWU v. Potter*, 343 F.3d 619, 623 (2d Cir. 2003) (quoting *Lunney v. United States*, 319 F.3d 550, 554 (2d Cir. 2003)). "Under Rule 12(b)(1), even 'a facially sufficient complaint may be dismissed for lack of subject matter jurisdiction if the asserted basis for jurisdiction is not sufficient.'" *Castillo v. Rice*, 581 F. Supp. 2d 468, 471 (S.D.N.Y. 2008) (quoting *Frisone v. PepsiCo Inc.*, 369 F. Supp. 2d 464, 469 (S.D.N.Y. 2005)).

To survive a Rule 12(b)(2) motion to dismiss, a plaintiff "bears the burden of demonstrating personal jurisdiction over a person or entity against whom it seeks to bring suit." *Penguin Gr. (USA) Inc. v. Am. Buddha*, 609 F.3d 30, 34 (2d Cir. 2010) (citation omitted). The plaintiff is required to make only "a prima facie showing" that jurisdiction exists. *Grand River Enters. Six Nations, Ltd. v. Pryor*, 425 F.3d 158, 165 (2d Cir. 2005) (citation omitted). At the pleading stage, such a showing "may be established solely by allegations" pleaded in good faith. *Dorchester Fin. Sec., Inc. v. Banco BRJ, S.A.*, 722 F.3d 81, 85 (2d Cir. 2013) (per curiam)).

Still, jurisdiction must be alleged with “factual specificity,” and conclusory statements will not suffice. *Jazini v. Nissan Motor Co.*, 148 F.3d 181, 185 (2d Cir. 1998).

Finally, to survive a motion to dismiss under Rule 12(b)(6) for failure to state a claim on which relief may be granted a plaintiff only needs to allege “sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

When considering any motion to dismiss a complaint under Rule 12, the Court must “‘accept[] all of the complaint’s factual allegations as true and draw[] all reasonable inferences in the plaintiff’s favor.’” *Siegel v. HSBC North America Holdings, Inc.*, 933 F.3d 217, 222 (2d Cir. 2019) (quoting *Giunta v. Dingman*, 893 F.3d 73, 78-79 (2d Cir. 2018)). However, the Court is “‘not bound to accept conclusory allegations or legal conclusions masquerading as factual conclusions.’” *Id.* (quoting *In re Facebook Initial Public Offering Derivative Litig.*, 797 F.3d 148, 159 (2d Cir. 2015)). The Court is limited to a “narrow universe of materials.” *Goel v. Bunge, Ltd.*, 820 F.3d 554, 559 (2d Cir. 2016). “Generally, [courts] do not look beyond ‘facts stated on the face of the complaint, . . . documents appended to the complaint or incorporated in the complaint by reference, and . . . matters of which judicial notice may be taken.’” *Id.* (quoting *Concord Assocs., L.P. v. Entm’t Props. Tr.*, 817 F.3d 46, 51 n. 2 (2d Cir. 2016)) (alterations in original).

DISCUSSION

Defendants make several arguments in favor of dismissal. First, Defendants argue that the Court does not have subject matter jurisdiction over this case because Defendants are entitled to “derivative foreign sovereign immunity.” *See* Def. Br. at 3-6. Defendants assert that, assuming the truth of Plaintiff’s Amended Complaint, it is alleged that GRA acted as agents of

the nation of Qatar. *See* Def. Br. at 3-6. Defendants also allege that the Court cannot assert jurisdiction over Plaintiffs' claims under the "prior pending action" doctrine. *See* Def. Br. at 6-7. Second, Defendants argue that at least some of the Defendants should be dismissed from the case for lack of personal jurisdiction. *See* Def. Br. at 7-10. Finally, Defendants allege that all of Plaintiffs' claims are insufficiently pleaded and fail to state a claim. *See* Def. Br. at 10-25.

I. The GRA Defendants Are Not Entitled to Derivative Foreign Sovereign Immunity

Defendants' first argument in support of dismissal, pursuant to Rule 12(b)(1), is that the GRA Defendants are entitled to derivative foreign sovereign immunity because, according to the Amended Complaint, GRA and its agents were acting as agents of the nation of Qatar when they hacked Plaintiffs' computer systems. *See* Def. Br. at 3-5. Plaintiffs urge the Court to follow the decision of the D.C. District Court in the parallel *Muzin* litigation and deny Defendants' motion for dismissal on the basis of derivative immunity. *See* Opp. at 3-8; *Muzin*, 2020 WL 1536350, at *7-8.

The Supreme Court has confirmed that while the Foreign Sovereign Immunities Act ("FSIA") governs the immunity of foreign nations to suit in American courts, individuals acting on behalf of foreign states may possess a derivative form of immunity under the common law. *Samantar v. Yousuf*, 560 U.S. 305, 322 (2010). Unlike status-based common law immunity that applies to any person who is a diplomatic representative of a foreign nation, *Muzin*, 944 F.3d at 442, Defendants here assert that they are entitled to "conduct-based" common law immunity because they were "agents [of a foreign nation] acting within the scope of their employment." *Moriah v. Bank of China Ltd.*, 107 F. Supp. 3d 272, 279 (S.D.N.Y. 2015). *Samantar* laid out a two-step procedure for determining whether a defendant is entitled to immunity based in the common law (as opposed to the FSIA). First, the Defendants are entitled to seek a "suggestion

of immunity” from the federal Department of State. *Samantar*, 560 U.S. at 311 (citing *Ex Parte Peru*, 318 U.S. 578, 581 (1943)). If the request is granted, the district court is deprived of jurisdiction. *Id.* (citing *Ex Parte Peru*, 318 U.S. at 588). However, absent such a request, the Court considers the second step and decides “whether all the requisites for such immunity exist[s]” while also considering “whether the ground of immunity is one which it is the established policy of the [State Department] to recognize.” *Id.* (citing *Ex Parte Peru*, 318 U.S. at 587, and then citing *Rep. of Mexico v. Hoffman*, 324 U.S. 30, 36 (1945)). Second Circuit law directs that common law foreign immunity extends only to defendants who either 1) committed acts in an “official capacity,” or where 2) “the effect of exercising jurisdiction would be to enforce a rule of law against the state.” *Heaney v. Gov. of Spain*, 445 F.2d 501, 504 (2d Cir. 1971) (citing Restatement of Foreign Relations Law of the United States § 66(f) (1965)).⁴

There cannot be significant dispute here that Defendants are not entitled to derivative immunity under this framework. While Defendants have not requested a “suggestion of immunity” from the State Department, the authorities cited by the Parties indicate that Defendants—U.S. citizens and companies—are not the type of defendants to whom State Department policy grants immunity. Plaintiff does not allege any facts that could be construed to show that Qatar ratified or approved of GRA’s hacking as would be required to make the hacking attacks actions taken in an “official capacity,” and Defendants have not provided any evidence either. Indeed, Defendants’ only argument that GRA’s actions are “official” is based on Plaintiffs’ allegation that Qatar directed GRA’s conduct. *See* Def. Br. at 4-5.

⁴ While the Second Circuit decision in *Heaney* pre-dates the Supreme Court’s decision in *Samantar*, the Supreme Court cited the decision as an example of a Circuit Court conducting the two-step immunity analysis outlined above. *See Samantar*, 560 U.S. at 312 (“Although cases involving individual foreign officials as defendants were rare, the same two-step procedure was typically followed when a foreign official asserted immunity.” (citing, among other cases, *Heaney*, 445 F.2d at 504-505)).

Defendants cite *Omari v. Khaimah Free Trade Zone Authority* in support of their argument. 2017 WL 3896399, at *10 (S.D.N.Y. Aug. 18, 2017). However, that case confirms that more facts are needed to confirm that actions taken at the direction of a government are, indeed, “official acts.” *See id.* at *10. In *Omari*, the plaintiff alleged particularized facts concerning an individual defendant’s use of specific UAE government apparatuses to arrest and jail the plaintiff. *Id.* These facts established that the actions were “undertaken through [] official channels and on behalf of [a government] in furtherance of its enforcement of its laws.” *Id.* Here, Plaintiffs have not alleged any facts, nor have Defendants made any representations, regarding the interaction between Qatari government officials or bodies and GRA. Instead, Plaintiffs have merely alleged a “covert unofficial policy” that does not establish “official” acts. *Doe v. Qi*, 349 F. Supp. 2d 1258, 1286 (N.D. Cal. 2004).⁵

The Court’s decision that Defendants here are not entitled to immunity also comports with evidence of the State Department’s position in similar cases. Specifically, the State Department previously has indicated that “U.S. residents . . . who enjoy the protections of U.S. law ordinarily should be subject to the jurisdiction of the courts, particularly when sued by U.S. residents.” *Yousuf v. Samantar*, 699 F.3d 763, 777-78 (4th Cir. 2012) (citing Statement of Interest of U.S. State Department). That position has been endorsed by at least one Circuit Court and at least two other District Courts as a basis on which to deny derivative immunity. *See id.* at 777-78 (affirming denial of a motion to dismiss and noting that “as a permanent legal resident, [Defendant] has a binding tie to the United States and its court system.”); *Muzin*, 2020 WL 1536350, at *6 (denying motion to dismiss on derivative immunity grounds and noting “the State Department would not grant immunity to these defendants [as American citizens], and no case

⁵ Defendants also do not establish, or even argue, that a judgment against them would effect a judgment on the nation of Qatar.

that the defendants have identified affects that conclusion.”); *ABI Jaoudi & Azar Trading Corp. v. Cigna Worldwide INS.. Co.*, No. 91-cv-6785, 2016 WL 3959078, at *18 (E.D. Pa. July 22, 2016) (“[Defendant’s] U.S. citizenship precludes him from claiming derivative foreign sovereign immunity.”).

The cases Defendants cite do not support their claim of derivative immunity. First, it cannot be argued that *Benomar*, Plaintiffs’ earlier case filed in this District regarding the same alleged conspiracy, addressed derivative immunity at all, because, as Judge Siebel noted in that case, the issue was not required for resolution of the case. *See* ECF No. 58 at 42:14-15, *Broidy Capital Mgmt, LLC v. Benomar*, No 7:18-cv-06615-CS (Jan. 2, 2019) (transcript of decision on the record). Second, each of the other cases to which Defendants point the Court involved some explicit adoption by a foreign government of actions of a non-U.S. citizen. *See Moriah*, 107 F. Supp. 3d at 276, 278-79 (former Israeli official was immune from deposition because, in part, Israel’s National Security Advisor confirmed to the court that any actions he took were “at the request” of a predecessor government official); *In re Terrorist Attacks on September 11, 2001*, 122 F. Supp. 3d 181 (S.D.N.Y. 2015) (Saudi Arabian government confirmed that Defendants were acting as “an official of the Saudi government” and were carrying out “core government functions”). Finally, Defendants have pointed the Court to no case where a court granted derivative sovereign immunity to a United States citizen, like all but one of Defendants here.

For these reasons, the Court finds that Defendants are not entitled to any form of derivative foreign sovereign immunity because the alleged hacks were not performed in an official capacity, as that term is defined for immunity purposes, and because any judgment would not affect Qatar. Moreover, absent a suggestion to the contrary in this case, the position of the State Department is to deny immunity to U.S. residents who allegedly acted on direction of a

foreign nation. As a result, the Court agrees with the *Muzin* court that Defendants are not entitled to derivative immunity and denies the motion to dismiss on this ground.

II. Plaintiffs Did Not Engage in Impermissible Claim-Splitting

Defendants also argue for dismissal, pursuant to Rule 12(b)(1), on the ground that Plaintiffs' claims in this case should have been raised in connection with the *Muzin* action since they share a "common nucleus of operative facts." Def. Br. at 6 (citing Complaint, ECF No. 1, ¶ 127). This argument is at odds with clear Second Circuit law.

The Second Circuit has confirmed the limits of the so-called "rule of duplicative litigation" or the "claim splitting rule." "[A] plaintiff has 'no right to maintain two actions on the same subject in the same court, against the same defendant at the same time.' In order for the rule to be properly invoked, however, 'the case must be the same.'" *Sacerdote v. Cammack Larhette Advisors, LLC*, 939 F.3d 498, 504 (2d Cir. 2019) (first quoting *Curtis v. Citibank, N.A.*, 226 F.3d 133, 139 (2d Cir. 2000), and then quoting *The Haytian Republic*, 154 U.S. 118, 124 (1894)). However, the Circuit also has clearly stated that "if a plaintiff suffers the same harm at the hands of two defendants, the plaintiff may institute one suit against one defendant and a separate suit against another defendant alleging that each caused his injury." *Id.* at 505 (citing *N. Assur. Co. of Am. v. Square D Co.*, 201 F.3d 84, 88–89 (2d Cir. 2000)).

There is an exception to the general rule allowing separate suits where the Defendants in the later-filed case are "in privity" with Defendants in the earlier-filed case. *Id.* at 505-507. Specifically, a later-filed case can still be precluded as duplicative for the same reasons and based on the same showing that would bind Defendants to a judgment under *res judicata* principles. *Id.* Among the facts bearing on whether Defendants are in privity, courts look to whether there exists

(1) agreements by a nonparty to be bound by the determination of issues in an action between others; (2) certain pre-existing substantive legal relationships based in property law between the nonparty and the party, such as preceding and succeeding owners of property, bailee and bailor, and assignee and assignor; (3) representative suits where the nonparty's interest was adequately represented by a party with the same interests, such as class actions and suits brought by trustees, guardians, and other fiduciaries; (4) when a nonparty has assumed control over the litigation in which the judgment was rendered; (5) when a nonparty is acting as a proxy, agent, or designated representative of a party bound by a judgment; and (6) when a statutory scheme expressly forecloses successive litigation by nonlitigants, so long as the scheme comports with due process.

Id. at 506 (citing *Taylor v. Sturgell*, 553 U.S. 880, 893-95 (2008)).

None of these factors is present here. No party has argued that Defendants here are sufficiently related to Defendants in the *Muzin* action such that GRA would be bound by a decision against Muzin or Stonington Strategies. Indeed, Defendants do not even argue that GRA “represent[s] the same interests” as Muzin and Stonington Strategies. *See Haytian Republic*, 154 U.S. at 124. Instead, Defendants merely have alleged that there are factual similarities or overlap between this case and *Muzin*. *See* Def. Br. at 6-7. This simply is not sufficient to warrant dismissal of this action.

The cases Defendants cite in their briefs for dismissal on duplicative litigation grounds again are readily distinguishable. In *Howard v. Klynveld Peat Marwick Goerdeler*, Defendants in a later filed action were deemed to represent the same interests as Defendants in an earlier-filed action because they were all partners in the same accounting firm, which was the counterparty of the employment contract at issue in both cases. 977 F. Supp. 654, 664 (S.D.N.Y. 1997). There is no relationship between GRA and Muzin comparable to the partnership agreement that bound the defendants in that case. Similarly, the newly-added Defendants in *Leptha Enterprises, Inc. v. Longenback* also were “contractual partners with mutual economic interests” when compared to defendants in a first-filed case. No. 90-cv-7704 (KTD), 1991 WL 183373, at *3 (S.D.N.Y. Sept. 9, 1991). There is no similar agreement alleged between

Defendants here and the *Muzin* defendants. Finally, while the decision in *7 West 57th Street Realty Co., LLC v. Citigroup, Inc.* supports Defendants’ assertion that co-conspirators are “in privity” for duplicative litigation purposes, *see* 2015 WL 1514539, at *27 (S.D.N.Y. Mar. 31, 2015), the Defendants there all acted in concert with each other toward a similar goal. *Id.* at *26. As alleged in this case, GRA and its agents acted to hack into Plaintiffs’ computer systems while the *Muzin* defendants allegedly subsequently publicized information resulting from the hacks. AC ¶¶ 88-92, 100-05, 106-15. The Amended Complaint does not allege any direct contact or coordination between Defendants in this case and the *Muzin* defendants similar to what was present in *Citigroup*. In fact, Plaintiffs specifically allege that GRA provided hacked documents to third parties and not to the *Muzin* defendants. *See* AC ¶¶ 100-05.

In sum, Plaintiffs have not improperly split their claims or engaged in duplicative litigation because the Defendants in this action are not in privity with the Defendants in *Muzin* and because the cases are not otherwise “the same.” As a result, Defendants’ motion to dismiss the Amended Complaint on these grounds is denied.

III. Plaintiffs Fail to Plausibly Allege that GRA was Responsible for the Hacks of Broidy’s Computer Systems

Defendants also move, pursuant to Federal Rule of Civil Procedure 12(b)(6), to dismiss the Amended Complaint for failure to state a claim. They argue that each of Plaintiffs’ ten claims fails to state a claim as a matter of law because the Amended Complaint does not tie any wrongdoing to GRA or any other Defendant. Because Plaintiffs have not alleged sufficient facts to plausibly support a reasonable inference that GRA or its agents were responsible for the hacks into Plaintiffs’ computer systems, Plaintiffs’ Amended Complaint is dismissed on these grounds.

Under Federal Rule of Civil Procedure 8, a plaintiff must state “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). The

Supreme Court, however, has interpreted the requirements of that rule to require that plaintiffs allege “sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 570). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of entitlement to relief.’” *Id.* (quoting *Twombly*, 550 U.S. at 557).

Plaintiffs’ Amended Complaint fails for the simple reason that it never plausibly connects the hacking activity to GRA or its agents. Plaintiffs’ primary allegations directly connecting Defendants to the hacks are based on the IP addresses Plaintiffs were able to capture from a forensic examination. *See* AC ¶¶ 96-98, 102-03. While most of the IP addresses that initiated the hacks were assigned to VPN providers and were thus anonymous, Plaintiffs were able to track an identifiable IP address for at least 14 different hacker log-ins to Plaintiffs’ servers. *See* AC ¶ 96. Those hacks originated in Vermont and Qatar, but Plaintiff does not allege any facts suggesting that it is plausible that the Vermont or Qatar addresses were used by GRA and not any other firm or person. Indeed, the only reference to the state of Vermont in the Amended Complaint is the identification of two IP addresses, and nothing related to Defendants. Similarly, the Amended Complaint alleges that the Gmail account belonging to Broidy’s Executive Assistant was accessed from an IP address located at a restaurant and event space in Harlem. AC ¶ 98. However, Plaintiffs never establish why that IP address make it plausible that GRA or its agents were behind the hacking.

Plaintiffs also attempt to link the alleged hacks to Defendants through an IP address affiliated with the Carolina Research and Education Network. *See* AC ¶ 102. Specifically, Plaintiffs allege that hacked documents were deposited into an email account (for dissemination to third parties) from an IP address registered to the “guest” WiFi network at the University of North Carolina (“UNC”). AC ¶ 102. Plaintiffs then allege that UNC is approximately one hour from Defendant GRA Maven’s office and also was the school where one of Defendant Kevin Chalker’s aides was taking classes at the time. AC ¶¶ 102-03. While these allegations do more to relate the activity to GRA, any purported link to Defendants is wholly speculative. As such, the facts alleged do not support that GRA is plausibly liable for hacking Plaintiffs’ systems.

Even if it is ultimately true that Qatar directed hacks against Plaintiffs, the Amended Complaint has not established a plausible case that GRA (as opposed to any other firm or person) actually executed the spear phishing campaign and theft of personal information from Plaintiffs. Plaintiff has provided no facts to establish that GRA or any of its employees is affiliated with the hacks of Plaintiffs’ computers. *See Tantaros v. Fox News Network, LLC*, No. 17 CIV. 2958 (GBD), 2018 WL 2731268, at *8 (S.D.N.Y. May 18, 2018) (granting motion to dismiss, in part because plaintiff “fail[ed] to plead any facts connecting the [Defendants] to an alleged sock puppet account that allegedly harassed Plaintiff.”); *see also Democratic Nat’l Comm. v. Russian Fed.*, 392 F. Supp. 3d 410, 432 (S.D.N.Y. 2019) (“[T]he DNC has not alleged that any defendant other than the Russian Federation participated in the hack of the DNC’s computers or theft of the DNC’s documents.”). As a result, the Plaintiff has not “plausibly” alleged that the hacks were committed by GRA.

Plaintiffs’ arguments to the contrary are unavailing. In their Opposition, Plaintiffs point to three types of allegations in the Amended Complaint “as to who executed the hacks and how.”

Opp. at 10. Specifically, Plaintiffs direct the Court to allegations that GRA has a relationship with Qatar and the “skill set” to carry out the attack (AC ¶¶ 42-51), then to allegations of communications between other alleged members of the conspiracy (AC ¶¶ 9-10, 120-21, 126-29), and finally to the allegation that GRA had an internal “special projects” division that was allegedly involved in previous Qatar-directed hacks (AC ¶¶ 6-7, 164, 174-187). None of these allegations provide support for the contention that GRA actually executed the hack in this case or otherwise suggest that GRA is plausibly liable.

At best, drawing reasonable inferences in Plaintiff’s favor, all Plaintiffs’ allegations regarding GRA’s “skill set” and the “special projects” division point only to the “feasibility” of the attack and GRA’s “capacity” to execute it—*i.e.* that GRA could have committed the attacks. That is legally insufficient to state a claim. *Tantaros*, 2018 WL 2731268, at *8 (“Plaintiff’s allegations at most support an inference that Defendants had the capability to intercept her communications. Such allegations, however, are insufficient to survive a motion to dismiss.”); *cf. Molefe v. Verizon New York, Inc.*, No 14-cv-1835-LTS-GWG, 2015 WL 1312262, at *4 (S.D.N.Y. Mar. 24, 2015) (granting motion to dismiss where Plaintiff alleged only the “feasibility” of tapping his telephone and not that it was actually accomplished by the defendants). Moreover, Plaintiffs’ allegations about communications between Qatari officials and other members of the alleged conspiracy, *see* AC ¶¶ 9-10, 120-21, 126-29, concern only defendants in the *Muzin* action and not Defendants here. While Plaintiffs have made out a strong case that GRA would be capable of hacking Plaintiffs’ systems, they have not presented any evidence that they did in fact do so. Indeed, Plaintiffs’ allegations about several IP addresses traceable to the hacks, *see* AC ¶¶ 96-99, 102-03, without providing any connection between GRA and these IP addresses, makes it less plausible that GRA had a role in the hacking attacks.

This conclusion is fatal to each of Plaintiffs' claims. All of the claims in the Amended Complaint are predicated on the supposition that Defendants hacked Plaintiffs' computer systems and disseminated the misappropriated documents to third parties. *See* AC ¶¶ 199, 216, 238, 256, 272, 280, 289, 298, 335-344, 410 (each cause of action including references to the alleged hacks). Indeed, Defendants' responsibility for the hacks and misappropriation of confidential information is at the heart of Plaintiffs' entire Amended Complaint. Absent allegations that in any way link GRA to the hacks, the Court cannot conclude that Defendants plausibly are liable for the injuries alleged in the Amended Complaint. *Iqbal*, 556 U.S. at 678. Instead, Plaintiffs have pleaded facts "consistent with" GRA's liability, but which "stop[] short of the line between possibility and plausibility of entitlement to relief." *Id.* (quoting *Twombly*, 550 U.S. at 557). As a result, the Court grants Defendants' motion to dismiss on this ground.⁶

CONCLUSION

For the reasons stated herein, although Defendants are not entitled to derivative sovereign immunity, the Court nonetheless GRANTS the motion to dismiss [ECF No. 72] Plaintiffs' Amended Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6). Put simply, Plaintiffs adequately allege that Defendants had the ability to commit the spear phishing and hack campaign alleged in the Amended Complaint, but not that they plausibly did so. The only identifiable facts about the hacks (e.g. IP addresses linked to a limited number of hacks) are not linked to Defendants in any way and cannot lead to a plausible inference of their liability. Thus,

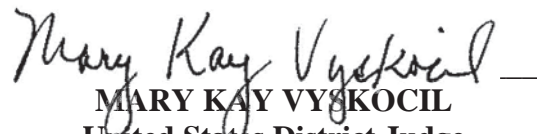
⁶ The Court does not address herein the Parties' arguments regarding personal jurisdiction or the arguments, pursuant to Rule 12(b)(6), why individual claims in the Amended Complaint fail to state a claim. *See* Def. Br. at 7-25. Because the Parties' arguments regarding jurisdiction depend in large part on whether Plaintiffs' RICO claims survive a motion to dismiss, judicial economy is served by reserving decision on those points pending the filing of any further amended complaint to address the deficiencies in Plaintiffs' claims as pleaded.

Plaintiffs' Amended Complaint is DISMISSED without prejudice. Defendants' request for oral argument [ECF No. 75] is denied as moot.

Because the Court dismisses the Amended Complaint on the basis of factual deficiencies, the Court is not in a position to decide whether further amendment would be futile or if Plaintiff could remedy the deficiencies through amendment. To the extent Plaintiffs intend to move for leave to file a Second Amended Complaint, the motion (together with a blacklined copy of the proposed Second Amended Complaint) should be filed within thirty days of this Opinion and Order.

SO ORDERED

Date: March 31, 2021
New York, New York


MARY KAY VYSKOCIL
United States District Judge